基于半量子秘密比较的量子拍卖协议

杨涵, 冯雁, 谢四江

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220500063

基于半量子秘密比较的量子拍卖协议

杨 涵[1] 冯 雁[1,2] 谢四江[1,2]
1 北京电子科技学院网络空间安全系 北京 100070
2 中国科学技术大学 合肥 230026
(3430127080@qq.com)

摘 要 针对量子密封拍卖协议中报价隐私保护不足、第三方不可信、对参与双方量子能力要求较高等情况,提出了一种将高能级单粒子作为信息载体的基于半量子秘密比较的量子密封投标拍卖协议。协议过程无需第三方参与,且采用半量子方式,仅要求拍卖方为强量子能力方,投标方仅需拥有反射粒子及制备单粒子的能力。协议利用半量子秘密比较,实现对投标方报价的隐私保护,拍卖方仅能获得报价之间的大小关系,而无法获取具体报价。文中通过理论分析证明了所提协议具有较高的安全性,能够抵御测量-重发攻击、截获-重发攻击、纠缠攻击、共谋攻击等多种攻击,且协议通信效率较稳定,不受投标人数的影响。

关键词:量子拍卖;量子密封投标拍卖;半量子;半量子秘密比较;高能级
中图法分类号 TN918.1

Quantum Auction Protocol Based on Semi-quantum Private Comparison

YANG Han[1],FENG Yan[1,2] and XIE Sijiang[1,2]
1 Cyberspace Security Department,Beijing Electronic Science and Technology Institute,Beijing 100070,China
2 University of Science and Technology of China,Hefei 230026,China

Abstract A quantum sealed-bid auction protocol using high-energy single particles as information carriers,based on semi-quantum private comparison is proposed to address the situation of insufficient privacy protection for quotations,the untrustworthy third party,and high quantum capability requirements for both participants in quantum sealed-bid auction protocols. This protocol does not involve third parties and uses a semi-quantum approach,requiring only that the auctioneer be a strong quantum capable party and that the bidder only have the ability to reflect particles and prepare single particles. This protocol achieves privacy protection for quotations through semi-quantum private comparison,where the auctioneer only has access to the size relationship between quotations,but not to specific quotations. It is theoretically analyzed that the protocol has high security and can resist the attacks of measure-resend,intercept-resend,entanglement,and collusion. And the communication efficiency of this protocol is stable,which is not affected by the number of bidders.

Keywords Quantum auction,Quantum sealed-bid auction,Semi-quantum,Semi-quantum private comparison,High-level quantum state

电子拍卖作为一种特殊的商品交易方式,是安全多方计算的一种实际应用。随着技术发展,依托于经典密码体系的传统电子拍卖方案在量子计算的冲击下将不再安全。

2009年,Naseri首次将量子技术运用到拍卖领域[1],通过GHZ态粒子实现报价的量子直接通信,但协议无法抵御双CNOT[2]、假粒子纠缠[3]、截获-重发[4]和共谋攻击[5]等攻击。2010年,Wang提出了基于Bell态的拍卖协议[6],但该协议仍无法抵抗CNOT和共谋攻击[7]。同年,Zhao等为抵御共谋攻击、确保报价的真实性,在文献[1]的基础上加入后确认机制[8],但由此带来了较高的通信复杂度,且仍无法预防竞标者串谋问题[9]。为降低后确认机制的复杂度,提高协议的安全性,Xu等于2011年在后确认阶段引入了Hash函数[10];He等于2012年更新了编码方案[11];2014年,Wang等应用了置换原理[12];2019年,Shi等将报价公布在公告板的方式替代后确认[13];同年,Wang等采用量子秘密共享降低后确认机制的复杂度[14];2020年,Zhang等实现了身份双向认证[15];同年,Liang通过对报价量子签名来确保其真实性[16]。此外,部分协议针对投标阶段提出了一些改进方案。2018年,Zhang等在投标阶段利用双模单光子提高了粒子利用率[17];2020年,Wang秘密比较报价信息,对报价使用经典线性加密[18];

到稿日期:2022-05-06 返修日期:2022-09-08
基金项目:安徽省量子通信与量子计算机重大项目引导性项目(AHY180500);广东省重点领域研发计划项目(2020B03030100001)
This work was supported by the Anhui Province Guidance Project of Quantum Communication and Quantum Computer Major Projects (AHY180500) and Guangdong Province Key Research and Development Project(2020B03030100001).
通信作者:冯雁(fengy@besti.edu.cn)

2022年，Shi运用中国剩余定理，实现了对报价的加密[19]，通过结合量子傅里叶变换通过向量形式比较报价[20]，通过引入量子安全多方分离确定报价区间[21]。上述协议[1-21]都要求参与方拥有完整的量子能力，且现有大部分协议存在对报价的隐私保护程度不够，协议过程需要可信或半可信第三方参与。

为增强拍卖报价隐私保护力度、削弱第三方的干扰，并降低对参与方的量子能力要求，本协议受文献[22]的启发，将两方的量子秘密比较扩展应用到拍卖过程的多方报价秘密比较，在此基础上提出了一种基于半量子秘密比较的量子拍卖协议，协议无需第三方参与，不仅能够实现对报价的隐私保护，还降低了对投标方的量子能力要求，安全性和通信效率也较好。

1 基础知识

1.1 高能级单粒子

协议中使用了高能级单粒子作为信息载体，高能级单粒子的具体定义如下：

d 维 Z 基单粒子定义为：$Z=\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\}$。

d 维 $\overline{X}$ 基单粒子定义为：$\overline{X}=\{F|0\rangle,F|1\rangle,\cdots,F|d-1\rangle\}$，其中 F 为量子傅里叶变换，$F|j\rangle=\frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1}\omega^{\delta j}|\delta\rangle$，$j=0,1,\cdots,d-1$，$\omega=e^{2\pi i/d}$。

当使用 d 维 Z 基测量一个 d 维 $\overline{X}$ 基光子，粒子将坍缩为 $\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\}$ 状态中的一种，且概率相等。

相比常规的二维量子态，高能级粒子的信息容量更大，从而具有更强的非局域性和量子信息处理能力，且能够增强量子密码方案的安全性，并提高量子逻辑门实现的效率[23]。虽然量子态的制备概率会随着维数的增加有明显降低，但通过相位交叉调制技术[23]、多芯光纤技术[24]等，能够实现制备高维度的量子态，且成功概率增大。

1.2 基于高能级单粒子态的半量子秘密比较

Xu[22]提出了基于高能级单粒子态的半量子秘密大小比较协议，协议在半可信第三方的全量子用户 TP 的帮助下，比较两位经典用户 Alice，Bob 的 N 位秘密信息 $X=\{x_1,x_2,\cdots,x_N\}$，$Y=\{y_1,y_2,\cdots,y_N\}$。协议过程如图 1 所示。

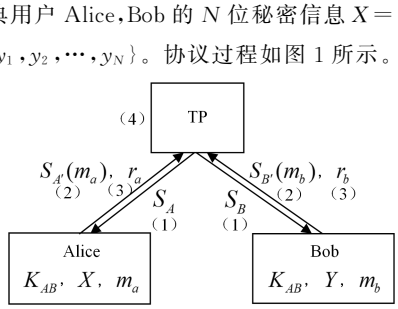


图 1 半量子秘密比较协议

Fig. 1 Semi-quantum private comparison protocol

(1)Alice 和 Bob 之间共享密钥 K_{AB}，TP 制备长度为 $16N(1+\sigma)$ 的高能级粒子，将其随机平分为两个序列 S_A 和 S_B，向 Alice(Bob)分发序列 $S_A(S_B)$。

(2)Alice(Bob)制备约 $4N$ 位高能级单粒子并记录初始状态为 $m_a(m_b)$，然后随机替换 $S_A(S_B)$ 中的粒子得到 $S_{A'}(S_{B'})$，并将其发送给 TP。经过窃听检测后，Alice(Bob)向 TP 公布替换粒子的位置信息，TP 通过测量，得到 Alice(Bob)掌握的信息 $m_a(m_b)$。

(3)Alice(Bob)通过计算 $r_a^i=m_a^i\oplus K_{AB}^i\oplus x_i$ ($r_b^i=m_b^i\oplus K_{AB}^i\oplus y_i$)，将自己的秘密信息 $X(Y)$ 嵌入 $r_a(r_b)$ 中，其中 $r_a^i(r_b^i)$ 表示 $r_a(r_b)$ 的第 i 位信息，并通过经典信道发送给 TP。

(4)由于 TP 同时拥有 m_a、m_b，TP 通过计算 $r_t^i=r_a^i\ominus r_b^i\ominus m_a^i\oplus m_b^i$，可知每位秘密信息 $X(Y)$ 每一位数据之间的大小关系：

$$\begin{cases} x_i<y_i, & h-1<r_t^i\leqslant 2h-2 \\ x_i=y_i, & r_t^i=0 \\ x_i>y_i, & 0<r_t^i\leqslant h-1 \end{cases} \tag{1}$$

2 基于半量子多方秘密比较求解最大值

在多个投标方的报价中找到最高报价是拍卖协议的关键。本文基于文献[22]提出的半量子秘密比较方案，提出了一种基于半量子多方秘密比较的求解最大值的方法。

若多位参与者 $B_i(i=1,2,\cdots,n)$ 分别持有 1 位秘密信息 $X_i(i=1,2,\cdots,n)$，半诚实可信第三方 TP 需要在 X_i 中找到最大值 $X_{\max}$。具体过程如图 2 所示。

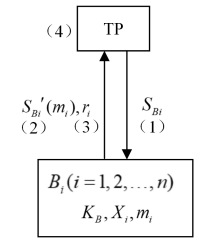


图 2 求取最大值

Fig. 2 Find the maximum value in the data

如图 2 所示，求解最大值 $X_{\max}$ 的过程基于文献[22]中基于高能级单粒子态的半量子秘密共享协议。首先，由半可信第三方 TP 制备长度大于 4 的粒子序列 $S_{B1},S_{B2},\cdots,S_{Bn}$ 分发给 $B_i(i=1,2,\cdots,n)$。B_i 将 S_{Bi} 中的粒子替换为制备的粒子态为 m_i 的粒子后发送给 TP。通过窃听检测后，B_i 公布替换位置，TP 通过测量可以得到 m_i。接着 B_i 将自己的秘密信息嵌入 r_i 中，$r_i=m_i\oplus K_B\oplus X_i$，并通过经典认证信道将 r_i 发送给 TP。

TP 通过 $r_t=r_i\ominus r_j\ominus m_i\oplus m_j$ 将数据两两分组进行比较，根据式(1)中 r_t 的值可知数据的关系，再通过如图 3 所示的晋级模式，得到多方数据中的最大值。若两个数据相等则两位数据同时晋级，若不相等，则数值大的数据晋级。

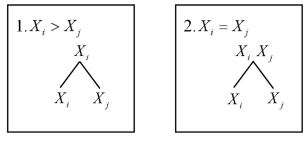


图 3 数据晋级模式

Fig. 3 Advancement model of data

重复上述过程，直至其中出现了最大值。最大值可以有多个。一轮完整的比较过程如图 4 所示。

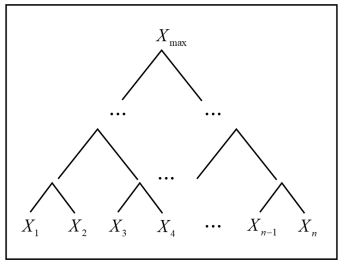


图 4　一轮比较的具体过程

Fig. 4　Specific process of a round of comparison

3　拍卖协议

本协议的参与方包括拍卖商 A 及 n 位投标者 $B_i(i=1,2,\cdots,n)$，投标者 $B_i(i=1,2,\cdots,n)$ 分别持有各自的投标价 $X_i(i=1,2,\cdots,n)$。协议规定拍卖商 A 为量子用户，投标者 $B_i(i=1,2,\cdots,n)$ 为经典用户。

本协议中的经典用户能够实施以下操作：1）不对粒子做任何操作，让粒子无干扰地反射；2）准备新的 Z 基粒子并发送给目标方[25-26]。

拍卖协议分为准备、投标、比较及公布 4 个阶段。准备阶段主要是参与方约定公共参数等信息，B_i 承诺自己报价的真实性；投标阶段主要是 B_i 向 A 发送包含报价的加密信息；比较阶段由 A 进行秘密比较，找出投标价中的最大值；公布阶段主要是 A 公布中标者 B_k，中标者公开中标价 X_k，A 以及 $B_i(i=1,2,\cdots,k-1,k+1,\cdots,n)$ 验证中标价的真实性。

3.1　准备阶段

步骤 1　拍卖商 A 和投标者 $B_i(i=1,2,\cdots,n)$ 之间约定安全参数 d 及一个抗碰撞的哈希函数 $H(*)$；投标者 $B_i(i=1,2,\cdots,n)$ 之间通过半量子密钥共享协议共享密钥 $K_B, K_B^i \in \{0,1,\cdots,t-1\}$。

步骤 2　投标者 B_i 生成一串随机数 str_i，根据共享的强碰撞 hash 函数，计算 h_i 并公告，除 B_i 外的人在 str_i 未知的情况下，无法通过 h_i 得知 X_i 的值。

$$h_i = H(str_i \oplus H(str_i \oplus X_i)) \tag{2}$$

步骤 3　投标者 B_i 将自己的报价 $X_i(i=1,2,\cdots,n)$ 转换成长度为 N 的 t 进制数，并进行拆分，$t=\frac{1}{2}(d+1)$，$\sum_{j=0}^{N-1} x_i^{(N-1)-j} \cdot t^j = x_i$，其中 $x_i^j \in \{0,1,\cdots,t-1\}$。

$$\begin{aligned} &X_i = \{x_i^0, x_i^1, \cdots, x_i^j, \cdots, x_i^{N-1}\} \\ &x_i^j \in \{0,1,\cdots,t-1\}, j=0,1,2,\cdots,N-1 \end{aligned} \tag{3}$$

3.2　投标阶段

步骤 4　拍卖商 A 生成 $4N(1+\sigma)\cdot n$ 个 d 维 $\overline{X}$ 基单粒子，即 $\overline{X}=\{F|0\rangle, F|1\rangle, \cdots, F|d-1\rangle\}$，$\sigma$ 是固定参数。A 将粒子随机平分为 n 份，并构建粒子序列 $S_{B1}, S_{B2}, \cdots, S_{Bn}$，再将 $S_{B1}, S_{B2}, \cdots, S_{Bn}$ 分别分发给投标者 B_i。

步骤 5　投标者 B_i 收到 S_{Bi} 后，产生一个随机二进制数 $R_{Bi}, R_{Bi}^j \in \{0,1\}^{4N(1+\sigma)}$，并根据随机数 R_{Bi} 进行对应的操作：若 $R_{Bi}^j=0$，则 B_i 对 S_{Bi} 的第 j 位粒子不做任何操作；若 $R_{Bi}^j=1$，则 B_i 将 S_{Bi} 的第 j 位粒子替换为其自己制备的一位 d 维 Z 基粒子后回传给 A，并记录新生成粒子的状态为 m_i；然后 B_i 将新形成的序列 S'_{Bi} 回传给 A。

$$S'_{Bi} = \{P_i^1, P_i^2, \cdots, P_i^{4N(1+\sigma)}\} \tag{4}$$

步骤 6　拍卖商 A 收到 S'_{Bi} 后，要求 B_i 公布 R_{Bi} 的值，并对 S'_{Bi} 进行窃听检测。当 $R_{Bi}^j=0$，则 A 使用 d 维 $\overline{X}$ 基对第 j 位粒子进行测量，若没有窃听者，则测量结果与 A 产生的初始状态相同。A 计算错误率，若高于阈值，则协议结束；否则协议继续，并丢弃用于窃听检测的粒子。将 $R_{Bi}^j=1$ 对应位置的粒子组成序列 S''_{Bi}，且粒子数量应大于 $2N$，否则协议结束。

步骤 7　拍卖商 A 从 S''_{Bi} 中随机选择 N 位粒子再次进行窃听检测。A 向 B_i 公布选中粒子的位置，B_i 分别告知 A 选中粒子的初始状态信息。然后，A 使用 d 维 Z 基测量选中粒子，并对比粒子初始状态计算错误率，若高于阈值，则协议结束；否则协议继续，丢弃用于窃听检测的粒子，剩余粒子组成序列 S'''_{Bi}。

步骤 8　投标者 B_i 从序列 S'''_{Bi} 中选择 N 位粒子，并将相应位置告知 A。B_i 将自己的报价信息嵌入 r_i^j 中，$r_i^j = m_i^j \oplus K_B^j \oplus x_i^j$，$j=0,1,\cdots,N-1$，并通过经典认证信道将 r_i^j 发送给 A。

步骤 9　拍卖商 A 根据 B_i 在步骤 5 中告知的位置信息，使用 d 维 Z 基测量相应的粒子，并记录测量结果为 M_i。A 可依次两两比较报价 x_i^j 的大小关系，例如，若想比较 X_a 和 X_b 的第 j 位数值的大小关系，则计算：

$$r_t = r_a^j \ominus r_b^j \ominus M_a^j \oplus M_b^j \tag{5}$$

其中，$\ominus$ 表示模 d 减，通过 r_t 可以得到相应的 r_c，从而得到相应的 X_a 和 X_b 的第 j 位数值的大小关系，具体转换关系如下：

$$r_c = \begin{cases} -1, & h-1<r_t<2h-2 \\ 0, & r_t=0 \\ 1, & 0<r_t\leqslant h-1 \end{cases} \Rightarrow \begin{cases} x_a^j < x_b^j, & r_c=-1 \\ x_a^j = x_b^j, & r_c=0 \\ x_a^j > x_b^j, & r_c=1 \end{cases} \tag{6}$$

3.3　比较阶段

步骤 10　由于 x_i^j 的上标 j 越小，x_i^j 对应的权重 $t^{(N-1)-j}$ 越大，这就意味这 j 越小时，x_i^j 越大，对应的 x_i 也就越大。因此，需要遍历 j 从 0 到 $N-1$，运用第 2 节求取最大值的方式，找到 j 相等的 $x_i^j(i=1,2,\cdots,n)$ 中的最大值，如图 5 所示。若一轮中的最大值有多个，此时 $j=j+1$，将上一轮得到的多个最大值对应的 x_i 再次进行比较，如图 6 所示，直至有且仅有一个最大值，此时该 x_i^j 的下标 i 对应的投标者 B_i 即为中标者，以下将中标者称为 $B_{\max}$。

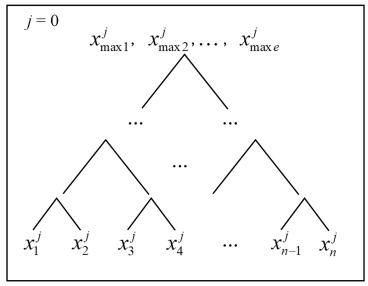


图 5　第一轮寻找最大值

Fig. 5　Looking for the maximum value in the first round

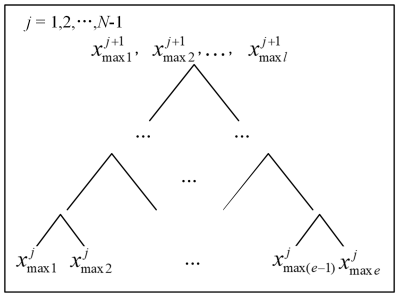


图 6 一轮寻找最大值

Fig. 6 Round of find the maximum value

3.4 公布阶段

步骤 11 拍卖商公布中标者为 $B_{\max}$，$B_{\max}$ 公开自己获得胜利报价的具体值 $X_{\max}$，同时公开 $str_{\max}$，所有人能够根据 $str_{\max}$ 和步骤 2 中公布的 $h_{\max}$ 的验证 $X_{\max}$ 的真实性，此时若其他投标者没有提出异议，则拍卖成功。协议的流程如图 7 所示。

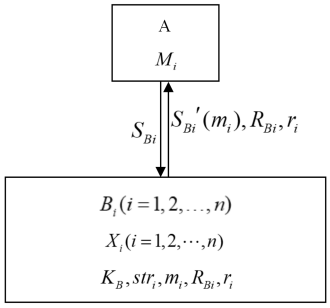


图 7 基于半量子秘密比较的量子拍卖协议

Fig. 7 Quantum auction protocol based on semi-quantum private comparison

4 安全性及通信效率分析

4.1 安全分析

本协议找到中标价的方式是基于 t 进制数的特性，将第 2 节求解最大值的方式执行多轮，求解找到出价最高的投标者。出价最高的投标者需公布自己的真实报价，即中标价，拍卖商和其他投标者能够校验该报价的真实性。拍卖商对报价的比较则运用了半量子秘密比较的方案，即拍卖商在收到了用于比较报价的数据信息后，仅能够通过计算 r_i^j 得到报价的大小关系而无法获得关于报价的具体值。由此可见，本协议实现了投标者报价隐私保护下的密封投标拍卖。

对协议的安全性分析，主要针对计算过程中受到测量-重发、截获-重发、纠缠及共谋攻击时，协议是否可以及时检测到攻击，以保证拍卖过程的安全性。

对于测量-重发、截获-重发、纠缠攻击，假设存在一位外部攻击者 Eve，希望获取或改变 A 与 B_i 之间的通信内容，且不被 A 和 B_i 发现。

4.1.1 测量-重发攻击

步骤 5 中，B_i 将新形成的序列 S'_{Bi} 回传给 A 的过程中，Eve 可能对序列 S'_{Bi} 进行测量重发攻击，即拦截 S'_{Bi} 并使用 d 维 Z 基测量序列中的粒子，并根据测量结果生成相同状态的新粒子替换原粒子，形成新的序列发送给 A。

B_i 收到序列 S'_{Bi} 后，根据随机产生一个二进制数 R_{Bi} 对序列粒子做对应操作。当 $R_{Bi}^j=0$ 时，B_i 对 S_{Bi} 的第 j 位粒子不做任何操作，此时第 j 位粒子的状态并未发生改变，Eve 的测量行为将导致粒子的坍缩，从而引入错误量。错误率超过阈值时，攻击将被发现，协议中止。因此，协议可以抵御测量-重发攻击。

4.1.2 截获-重发攻击

步骤 4 中，A 将粒子序列 $S_{B1}, S_{B2}, \cdots, S_{Bn}$ 分发给投标者 B_i 的过程中，Eve 可能对序列 S_{Bi} 进行截获重发攻击，即拦截传输的序列 S_{Bi} 并生成与序列相同长度的伪序列，随后发送给对应的 B_i。假设 Eve 预先准备的伪序列的制备基都为 Z 基，在步骤 5 中，B_i 随机生成 R_{Bi}，当 $R_{Bi}^j=0$ 时，不对第 j 位粒子做任何操作，直接返回给 A，Eve 的行为将导致错误量的引入；当 $R_{Bi}^j=1$ 时，在步骤 7 中，A 将从剩余的粒子序列 S''_{Bi} 中随机选择 N 位粒子再次进行窃听检测。由于 Eve 没有 m_i 的相关信息，Eve 的攻击仍将不可避免地引入错误量，因此协议可以抵御截获重发攻击。

4.1.3 纠缠攻击

在步骤 5 中，B_i 将新形成的序列 S'_{Bi} 回传给 A 的过程中，本协议应对纠缠攻击的方式与 Xu 相似，若 Eve 进行纠缠攻击，即对序列 S'_{Bi} 进行酉操作 U_E，并制备虚假粒子 $|\varepsilon\rangle$ 作为附属空间，具体如式(7)所示，Eve 能够通过测量 $|\varepsilon\rangle$ 得到 B_i 的相关信息后，再将序列 S'_{Bi} 发送给 A[22]。

$$|k\rangle \xrightarrow{\text{纠缠攻击}} U_E|k\rangle|\varepsilon\rangle_E=\sum_{\delta=0}^{d-1}\lambda_{k\delta}|\delta\rangle|E_{k\delta}\rangle_E \tag{7}$$

$$\begin{aligned}&|j_v\rangle=F|v\rangle \xrightarrow{\text{纠缠攻击}} U_E|j_v\rangle|\varepsilon\rangle_E\\&U_E|j_v\rangle|\varepsilon\rangle_E=\frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1}\omega^{\delta v}\lambda_{\delta\delta}|\delta\rangle|E_{\delta\delta}\rangle_E\end{aligned} \tag{8}$$

由量子逆傅里叶变换，可得 $|\delta\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\omega^{-j\delta}|k_j\rangle$，带入式(8)可得[22]：

$$U_E|J_v\rangle|\varepsilon\rangle_E=\frac{1}{d}\sum_{u=0}^{d-1}\left(|J_u\rangle\sum_{\delta=0}^{d-1}\omega^{\delta(v-u)}\lambda_{\delta\delta}|E_{\delta\delta}\rangle_E\right) \tag{9}$$

由式(9)可知，当且仅当 $v\neq u$ 时，$\sum_{\delta=0}^{d-1}\omega^{\delta(v-u)}\lambda_{\delta\delta}|E_{\delta\delta}\rangle_E=0$，$u=0,1,\cdots,d-1$ 攻击才不会被发现。此时，由于 $\sum_{\delta=0}^{d-1}\omega^{\delta(v-u)}=0$，可得 $\lambda_{00}|E_{00}\rangle_E=\lambda_{11}|E_{11}\rangle_E=\cdots=\lambda_{(d-1)(d-1)}|E_{(d-1)(d-1)}\rangle_E$，Eve 仍旧无法区分 $\lambda_{00}|E_{00}\rangle_E$，$\lambda_{11}|E_{11}\rangle_E$，$\cdots$，$\lambda_{(d-1)(d-1)}|E_{(d-1)(d-1)}\rangle_E$[22]。

因此，本协议可以抵御纠缠攻击。

4.1.4 共谋攻击

由于本协议在 Xu 的基于高能级单粒子的半量子秘密比较协议的基础上引入了 hash 函数用于后确认，降低了对拍卖方的诚信要求，这就导致协议还可能面临共谋攻击。针对本协议的共谋攻击，主要指恶意投标者与拍卖方之间的共谋。

假设存在恶意投标者 B_e 与拍卖方共谋，将 B_e 公布为虚假的中标者，此时 B_e 需要公开自己的报价及 str_e。

(1)若 B_e 公布自己的真实报价 X_e，那么价格更高的投标者会提出质疑。

(2)若 B_e 谎称自己的报价为 X_e'，由于拍卖方和 B_e 都不知道报价的具体内容，因此无法保证 X_e' 就是所有报价中的最大值。即便 X_e' 就是最大值，此时，其他投标者可以根据 B_e

公开的随机数 str_e 和 X_e' 得到对应的 h_e'，由于哈希函数抗碰撞的特性，难以找到 $X_e' \neq X_e$ 时 $h_{emax}=h_e$，通过计算不难发现：$h_e' \neq h_e$。

因此，本协议可以抵御共谋攻击。

4.2　通信效率分析

本协议的通信效率的计算式如下：

$$\eta=\frac{c}{t}\times 100\% \tag{10}$$

其中，c 表示传输信息的比特数，t 表示所有参与者生成的粒子总数。假设协议有 n 位投标者 B_i，需要传输报价的粒子总数为 $c=N\cdot n$。为实现 c 的传输，步骤 4 中 A 需要生成 $t_1=4N(1+\sigma)\cdot n$ 位粒子，步骤 5 中 n 位 B_i 将分别生成 $2N$ 位粒子，即 $t_2=2N\cdot n$ 位粒子，总计 $t=t_1+t_2=4N(1+\sigma)\cdot n+2N\cdot n \Rightarrow 6N\cdot n$。综上可知，本协议的通信效率为 $\eta=(n\cdot N)/(n\cdot 6N)\times 100\% \approx 16.67\%$。

对比一些已有的量子拍卖协议不难发现，当参与投标的人数较少时，本协议的通信效率低于其他拍卖协议，但随着参与投标的人数上升，本协议的通信效率能够超过部分量子拍卖协议，虽然仍旧低于部分协议，但本协议采用半量子，降低了对投标方量子能力的要求，使得操作简化，适用性较高。表 1 列出了本协议与几种经典拍卖协议的比较分析结果，其中 n 表示参与拍卖的投标方人数。

表 1　几种量子拍卖协议的对比

Table 1　Comparison of several quantum auction protocols

	Zhao's Method[8]	Liang's Method[15]	Luo's Method[27]	This Method
information carriers	GHZ	Single particle	Bell	High-level quantum state
Bidders quantum capacity	All	All	All	reflect particles and prepare single particles
Information sent	Real	Real	Real	Encrypted
Privacy	Weak	Weak	Weak	Strong
Efficiency	$1/n$	20%	$1/(n+1)$	16.67%

结束语　本协议结合半量子秘密比较，将涉及双方的协议扩展应用于多方报价的大小比较，使得拍卖方仅能获得报价的大小关系，而无法得知报价的具体内容，实现了对报价的隐私保护。协议过程仅涉及拍卖方和投标方，不需要第三方参与；且基于半量子环境，降低了对投标方量子能力的要求。通过理论分析证明了本协议能够及时发现并抵御测量-重发，截获重发、纠缠、共谋等攻击，安全性较好。与同类型量子拍卖协议相比，本协议的通信效率不会受投标人数的影响，且效率较高。

参 考 文 献

[1] NASERI M. Secure quantum sealed-bid auction [J]. Optics Communications, 2009, 282(9): 1939-1943.

[2] QIN S J, GAO F, WEN Q Y, et al. Cryptanalysis and improvement of a secure quantumsealed-bid auction [J]. Optics Communications, 2009, 282(19): 4014-4016.

[3] YANG Y G, NASERI M, WEN Q Y. Improved secure quantum sealed-bid auction [J]. Optics Communications, 2009, 282(20): 4167-4170.

[4] LIU, Y M, WANG D, LIU X S, et al. Revisiting Naseri's Secure Quantum Sealed-bid Auction [J]. International Journal of Quantum Information, 2009, 7(6): 1295-1301.

[5] ZHENG Y Q, ZHAO Z W. Comment on: "Secure Quantum Sealed-bid Auction" [J]. Optics Communications, 2009, 282(20): 4182.

[6] WANG Z Y. Quantum Secure Direct Communication and Quantum Sealed-Bid Auction with EPR Pairs [J]. Communications in Theoretical Physics, 2010, 54(6): 997-1002.

[7] LIU W J, WANG F, JI S, et al. Attacks and Improvement of Quantum Sealed-Bid Auction with EPR Pairs [J]. Communications in Theoretical Physics, 2014, 61(6): 686-690.

[8] ZHAO Z W, NASERI M, ZHENG Y Q. Secure quantum sealed-bid auction with post-confirmation [J]. Optics Communications, 2010, 283(16): 3194-3197.

[9] ZHAO Z J, WANG W J. Comment on: "Cryptanalysis and Improvement of the Secure Quantum Sealed-bid Auction with Post Confirmation" [J]. International Journal of Quantum Information, 2014, 12(6): 1475001-1-1475001-3.

[10] XU G A, ZHAO Z W, CHEN X B, et al. Cryptanalysis and improvement of the secure quantum sealed-bid auction with post-confirmation [J]. International Journal of Quantum Information, 2011, 9(6): 1383-1392.

[11] HE L B, HUANG L S, YANG W, et al. Cryptanalysis and Melioration of Secure Quantum Sealed-bid Auction with Post-confirmation [J]. Quantum Information Processing, 2012, 11(6): 1359-1369.

[12] WANG Q L, ZHANG W W, SU Q. Revisiting "The Loophole of the Improved Secure Quantum Sealed-Bid Auction with Post-Confirmation and Solution" [J]. International Journal of Theoretical Physics, 2014, 53(9): 3147-3153.

[13] SHI R H, LIANG F Y, WANG Q, et al. An Effective Quantum Sealed-bid Auction Protocol [J]. Netinfo Security, 2019, 19(8): 44-50.

[14] WANG Q, SHI R H, CHEN Z K, et al. A Quantum Sealed Auction Protocol Based on Secret Sharing [J]. International Journal of Theoretical Physics, 2019, 58(4): 1128-1137.

[15] SHI R H, ZHANG R, LIU B, et al. Cryptanalysis and Improvement of Quantum Sealed-Bid Auction [J]. International Journal of Theoretical Physics, 2020(59): 1917-1926.

[16] LIANG F Y. Design of a Verifiable Bidding auction Protocol for Quantum Seals [D]. Hefei: Anhui University, 2020.

[17] ZHANG R, SHI R H, QIN J Q, et al. An Economic and Feasible Quantum Sealed-bid Auction Protocol [J]. Quantum Information Processing, 2018, 17(2): 35-1-35-14.

[18] WANG Q. Research on privacy protection and post confirmation

mechanism of quantum sealed bidding auction[D]. Hefei: Anhui University, 2020.

[19] SHI R H. Quantum Sealed-Bid AuctionWithout a Trusted Third Party [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021, 68(10): 4221-4231.

[20] SHI R H. Anonymous Quantum Sealed-Bid Auction [J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69(2): 414-418.

[21] SHI R H, LI Y F. A Feasible Quantum Sealed-Bid Auction Scheme Without an Auctioneer [J]. IEEE Transactions on Quantum Engineering, 2022(3): 1-12.

[22] XU Q D. Design and analysis of a two-party semi-quantum secret comparison protocol[D]. Nanchang: Nanchang University, 2021.

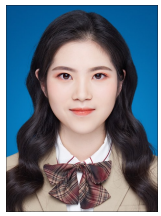
[23] YE X L. Generation of high-dimensional quantum entangled states and its application in quantum communication [D]. Xiamen: Huaqiao University, 2013.

[24] HU X M, XING W B, LIU B H, et al. Efficient generation of high-dimensional entanglement through multipath down-conversion [J]. Physical Review Letters, 2020, 125(9): 090503-1-090503-6.

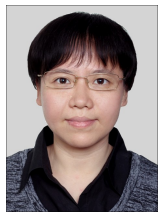
[25] BOYER M, KENIGSBERG D, MOR T. Quantum key distribution with classical Bob [J]. Physical Review Letters, 2007, 99(14): 140501-1-140501-4.

[26] NIE Y Y, LI Y H, WANG Z S. Semi-quantum information splitting using GHZ-type states [J]. Quantum Information Processing, 2013, 12(1): 437-448.

[27] LUO Y, ZHAO Z W, ZHAO Z J, et al. The loophole of the Improved Secure Quantum Sealed-bid Auction with Post-confirmation and Solution [J]. Quantum Information Processing, 2013, 12(1): 295-302.



YANG Han, born in 1998, postgraduate. Her main research interests include cyberspace security and quantum cryptography.



FENG Yan, born in 1979, master, associate professor. Her main research interests include cryptography, network security, and quantum communication network security system.

(责任编辑:喻藜)